

# SECRET INFORMATION MANAGEMENT SCHEME BASED ON SECRET SHARING SCHEME

**Publication number:** WO2005076518 (A1)

**Publication date:** 2005-08-18

**Inventor(s):** KAGAYA MAKOTO; OGIHARA TOSHIHIKO; NOMURA SUSUMU +

**Applicant(s):** NTT COMM CORP [JP]; KAGAYA MAKOTO; OGIHARA TOSHIHIKO; NOMURA SUSUMU +

**Classification:**

- **international:** **H04L9/08; H04L9/08;** (IPC1-7): H04L9/08

- **European:** H04L9/08R; H04L9/08S

**Application number:** WO2005JP02514 20050210

**Priority number(s):** JP20040033352 20040210; JP20040033355 20040210; JP20040169001 20040607

**Also published as:**

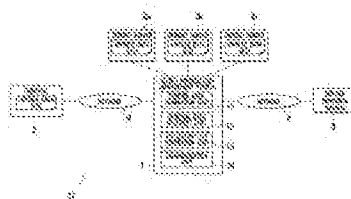
US2007160197 (A1)  
EP1714423 (A1)

**Cited documents:**

US6411716 (B1)  
EP0723348 (A2)  
US5675649 (A)  
US6209091 (B1)

## Abstract of WO 2005076518 (A1)

In a secret information management system for managing a secret information of a user, the secret information is divided into a plurality of divided data by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data, and a part of the plurality of divided data is stored into a terminal of the user as user's divided data while a rest of the plurality of divided data are stored into one or more of deposit servers. Then, a plurality of re-divided data different from the plurality of divided data are generated, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme, and a part of the plurality of re-divided data is stored into the terminal as newly generated user's divided data while a rest of the plurality of re-divided data are stored into the deposit servers as newly generated divided data.



Data supplied from the **espacenet** database — Worldwide